IN THE CLAIMS

1. (Previously Presented) System for providing encrypted data to be used in a content player comprising a decryption device, comprising:

an encryption device for encrypting data using an encryption algorithm,

a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and

a control device for providing a protected contents structure containing the encrypted data, the secure device data, said protocol information and attribute data for finding relevant parts inside the protected contents structure,

wherein the attribute data comprises information to find in the protected contents structure information on an appropriate protocol for establishing a communication interface between the content player and the secure device for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data.

2. (Original) System according to claim 1, wherein said protection device provides at least one security device applet containing said information on a protocol for communication.

3. (Previously Presented) System for decrypting encrypted data in a content player, comprising:

an input for receiving protected contents containing encrypted data, secure device data, information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and attribute data for finding relevant parts inside the protected contents,

a decryption device, and

a control device,

wherein said secure device data comprises the information required to decrypt the encrypted data, and wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player

and the secure device for retrieving the information required to decrypt the encrypted data, wherein the control device is programmed to use the attribute data to find the appropriate protocol information to establish a communication interface between the decryption device and a secure device used with the content player,

wherein the decryption device is suitable for communicating with the secure device as controlled by the protocol information to obtain the information required by the decryption device to decrypt the encrypted data and generated by the secure device by transforming secure device data communicated to the secure device through the communication interface.

4. (Previously Presented) System according to claim 3, wherein said information on the appropriate protocol for communication between the content player and the secure device is provided as a secure device applet, wherein the control device is programmed to operate as a virtual machine to execute the secure device applet to establish said communication interface.

5. (Previously Presented) System according to claim 4, wherein at least one secure device applet in the protected contents is authenticated, wherein the control device comprises an applet loader for verifying the authentication of a secure device applet, wherein only a verified secure device applet is loaded into the virtual machine.

6. (Previously Presented) System according to claim 5, wherein at least one secure device applet in the protected contents is encrypted, wherein the applet loader is suitable for decrypting an encrypted secure device applet.

7. (Previously Presented) System according to claim 4, wherein the virtual machine comprises a content player application program interface and a security application program interface, the secure device applet communicating with the content player and the secure device by means of said content player application program interface and said security application program interface, respectively.

8. (Previously Presented) System according to claim 4, wherein the control device is arranged to determine of which type the secure device used in the system is, wherein the control device is arranged to retrieve a secure device applet from the protected contents corresponding with the determined type of secure device.

9. (Previously Presented) System according to claim 4, wherein the system is part of a content player connected to a network, wherein the control device is arranged to determined the type of secure device used in the system, and wherein the control device is arranged to request a corresponding secure device applet to be downloaded from a service provider.

10. (Previously Presented) Method for providing a communication interface between a decryption device and a secure device in a content player, comprising:

receiving a protected contents structure containing secure device data, information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, and attribute data for finding relevant parts inside the protected contents structure, wherein said secure device data comprises the information required to decrypt the encrypted data, the attribute data comprising information to find in the protected contents structure information on an appropriate protocol for communication between the content player and the secure device for retrieving the information required to decrypt the encrypted data, and

retrieving said protocol information from the protected contents structure to establish a communication interface between the decryption device and a secure device used with the contents player to transform secure device data communicated to the secure device through the communication interface into information required by the decryption device to decrypt encrypted data.

11. (Original) Method according to claim 10, wherein said protocol information is provided as a secure device applet, wherein the secure device applet is executed in a virtual machine to establish the communication interface.

12. (Previously Presented) Method according to claim 10, further comprising detecting which type of secure device is being used with the content player, and requesting corresponding protocol information or a secure device applet from a source providing the protected contents structure.

13. (Previously Presented) Method according to claim 10, further comprising detecting which type of secure device is being used with the content player, and requesting corresponding protocol information or a secure device applet from a source providing the protected contents structure.

14. (Previously Presented) Method according to claim 10, wherein said protocol information or secure device applet is authenticated, further comprising verifying the authentication, and using only verified protocol information or a verified secure device applet to establish said communication interface.

15. (Previously Presented) Method for broadcasting protected contents, comprising:

encrypting data using an encryption algorithm,

providing secure device data,

providing information on a protocol for establishing a communication interface between a content player and a secure device arranged to transform the secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data,

providing protected contents containing the encrypted data, the secure device data, the protocol information and attribute data, and

broadcasting the protected contents,

wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and the secure device.